Tomcat ROOT 계정으로 기동 시 Permission Denided 이슈

→ 2/2 09:35부터 14:55까지 서블릿 호출에서 ***java.io.ClassNotFountException, java.io.FileNotFoundException(허가 거부) 에러*** 가 발생

Tomcat을 ROOT 계정으로 기동 시 발생한 문제점

Listener 설정

이 옵션은 tomcat이 기동할 때, root 사용자이면 기동을 하지 못하게 하는 옵션이다. 서버를 운영해본 사람이라면 종종 겪었을 실수중의 하나가 application server를 root 권한으로 띄웠다가 다음번에 다시 실행하려고 하면 permission 에러가 나는 시나리오 이다. root 권한으로 서버가 실행되었기 때문에, 각종 config 파일이나 log 파일들의 permission이 모두 root로 바뀌어 버리기 때문에, 일반 계정으로 다시 재 기동하려고 시도하면, config 파일이나 log file들의 permission 이 바뀌어서 파일을 읽어나 쓰는데 실패하게 되고 결국 서버 기동이 불가능한 경우가 있다. 이 옵션은 이러한 실수를 막아 줄 수 있다.

→ *Application Server*를 기존 osaka 계정이 아닌 ROOT 계정으로 띄우게 되면 war 파일이 풀린 디렉토리, Log, config 디렉토리 내의 일부 파일들의 권한이 ROOT 로 변경된다. (정확하게 어떤 파일이 변경되는지는 확인하지 못했습니다. 추가적으로 확인해보도록 하겠습니다)

따라서 이 후 osaka 계정으로 Tomcat을 기동해도, 빌드 과정의 class 파일을 찾는 과정에서 ***ClassNotFoundException (컴파일된 class 파일을 찾을 수 없다), FileNotFoundException, Permission Denied (찾았지만 권한이 없음)*** 을 발생시킨다.

→ 위와 같은 문제를 방지하기 위해 server.xml 의 설정을 통해서 ROOT 계정으로 Tomcat을 기동시키는 것을 막는 설정입니다.

```
<!-- 톰캣을 루트 사용자로 실행하지 않도록 막아준다. 루트로 톰캣을 실행할 경우 로그등이 루트권한으로 저장되어 문제가 발생할 수 있기 때문 -->
<Listener className="org.apache.catalina.security.SecurityListener" checkedOsUsers="root" />
```

The following additional attributes are supported by the **Security Lifecycle Listener**:

Attribute	Description
checkedOsUsers	A comma separated list of OS users that must not be used to start Tomcat. If not specified, the default value of **root** is used. To disable this check, set the attribute to the empty string. Usernames are checked in a case-insensitive manner.

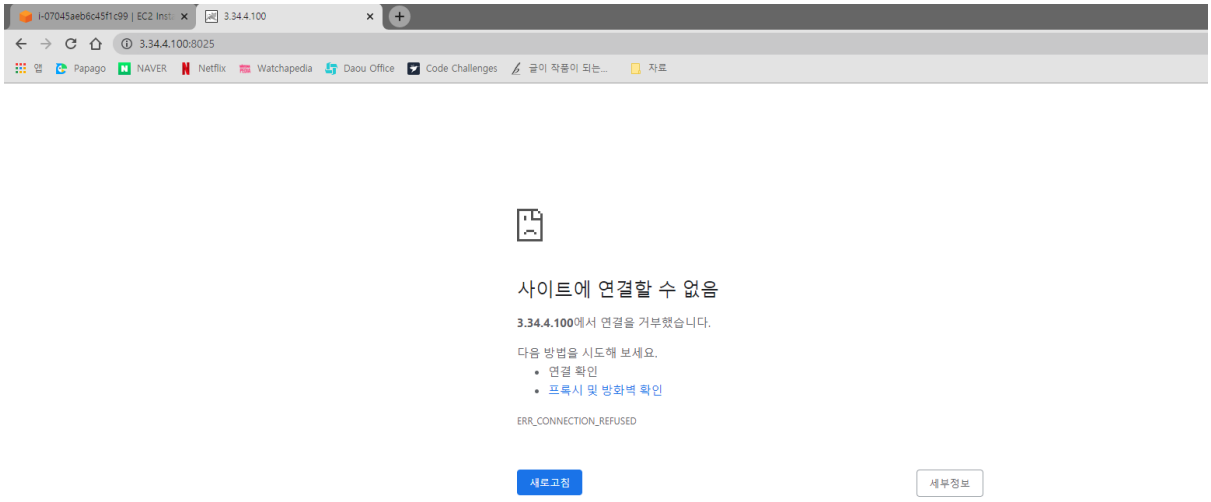
위에서 언급한 *tomcat listener(Security Lifecycle Listener)의 checkOSUsers*의 설명.

해당 파라미터에 문자열(','로 구분)을 입력하여 톰캣 실행을 차단하는 목록을 만들 수 있음 (최초 *server.xml* 내에서는 주석 처리가 되어있다). 또한 umask의 사용 여부에 따라 <Listenr> 태그 외에도 *$CATALINA_HOME/bin/catailina.sh* 에서 umask를 얻는 행도 주석처리를 제거해야 사용할 수 있음

> 💡 *umask : default로 지정되어 있는 파일, 디렉토리별 권한을 custom하기 위해 조정하는 값*
> *https://jhnyang.tistory.com/63*

→ 실제로 해당 옵션을 통해 ROOT 계정의 차단 여부는 EC2 계정을 생성해 테스트해보았습니다.

1. root 계정으로 Tomcat을 구동하여 정상적으로 구동되는지 확인
2. shutdown 이후 server.xml (25) 라인의 ***<Listener className="org.apache.catalina.security.SecurityListener" checkedOsUsers="root" (추가)/>*** 을 추가(주석 풀기 + checkOsUsers 파라미터 추가) 한 뒤 Tomcat 기동
3. 해당 라인을 추가한 경우 ec2-user 계정에서는 Tomcat이 정상적으로 띄워지지만, root 계정으로 Tomcat을 띄우면 서버 호출 시 서버에서 연결을 차단한다.



참고자료 : https://ejjoo.github.io/server/2019/12/22/tomcat.html, https://blog.codeoctopus.net/110